Remarks/Arguments

Reconsideration of this application is requested.

Claim Status

Claims 1-23 are pending in this application. Since this response does not amend, add or cancel any claims, no listing of claims is required under 37 CFR 1.121(c).

Claim Rejections – 35 USC 102(b)

Claims 1, 2, 4 and 12-23 are rejected under 35 USC 102(b) as anticipated by Tanaka "Security Certified Identity-based Non-Interactive Key Sharing". Applicant respectfully traverses this rejection and asserts that claims 1, 2, 4 and 12-23 include limitations not disclosed by Tanaka, and therefore cannot be anticipated by Tanaka.

Tanaka specifically teaches mapping onto a finite field based on ID information. In contrast, claims 1, 2, 4 and 12-23 of the present invention recite mapping on an algebraic curve based on ID information.

According to Tanaka, equations (3) and (4) take a form of raising a primitive element g on a finite field F_q with a hash value (integral value) of ID information. Tanaka's method has safety problems in that a secret key of a key generation center can be revealed by users in collusion, or a secret key of a third party user who is not involved in the collusion can be calculated. Moreover, the g of Tanaka is common to all users, and a key is generated by the power method of Tanaka using a hash value of ID information. Tanaka's equations specifically teach a mapping indicating the correspondence $h(ID_A)P$ with respect to a point P. This teaching of Tanaka is different from the mapping proposed by the present invention.

In contrast, the mapping method of the present invention obtains a point on an algebraic curve based on ID information. The point on the algebraic curve is expressed as a two dimensional value, which is specifically a point on a projective plane. The claimed mapping method of the present invention does not produce the same values if used with the method of Tanaka. For example, if the mapping method of the present invention is applied to a primitive element of a finite field of

Tanaka, g_A is obtained as a mapping destination of ID information. To share a key using this g_A, it is necessary to calculate an x to satisfy the equation $g_A=g^x$. This requires solution of a discrete logarithm problem, which is unlikely when a safe parameter is set. The present invention, in contrast to Tanaka, makes this possible using an algebraic curve. A bilinear type mapping, such as Weil Pairing, can be used in calculating a shared key in the present invention.

Since Tanaka does not disclose each and every element of claims 1, 2, 4 and 12-23, it cannot anticipate those claims. Thus, the rejections under 35 USC 102(b) should be withdrawn.

Claim Rejections – 35 USC 103(a)

Claims 3, 5, 6 and 8-11 are rejected under 35 USC 103(a) as obvious over Tanaka in view of Miyaji (USPN 5,272,755). Since Miyaji does not disclose or suggest using Weil pairing for its cryptosystem, applicant respectfully traverses these rejections and asserts that claims 3, 5, 6 and 8-11 are not rendered obvious by Tanaka and Miyaji. Miyaji merely refers to an MOV attack, which represents one method of attacking an elliptic curve cryptosystem.

With reference to claims 3 and 9, paragraph 17 of the Action asserts that Miyaji "teaches a one-way elliptical curve function based public key cryptosystem using Weil pairing". Applicant disagrees. Weil pairing is mentioned in evaluation of safety against a MOV attack, and the MOV attack is slightly extended for more accurate safety evaluation. The teachings of the prior art suggest a method that can be expressed as $h(ID_A)P$, which corresponds to $g^{h(ID_A)}$ of Tanaka. By using the expression $h(ID_A)P$ on the basis of the method of Tanaka, it is possible to share a key, but the safety against a collusion attack is impaired.

As a result, if the mapping method of the claimed invention were realized on an elliptic curve used for constructing an encryption system as disclosed in Miyaji, it would be unlikely to calculate Weil pairing (Miyaji uses an elliptic curve that defies a MOV attack) and, therefore, highly unlikely to share a key. Moreover, if a

discrete logarithm problem on an elliptic curve were solved, the safety of the cryptosystem itself would be ineffective, or in some cases ruined.

With reference to claims 6 and 11, paragraphs 19 and 22 of the Action cite the equation $K=B^a=a^b$ in FIG. 1 of Miyaji. However, the referenced equation is, to be correct, $K=\beta^a=\alpha^b$, wherein $\alpha= g^\alpha$ is not the same with a, and $\beta=g^b$ is not the same with b. The Action asserts that "Inverse numeric values are generated in a process in respective entities when sharing the key/common key generation". Applicant disagrees and does not understand what values in Miyaji correspond to the claimed "inverse numeric values" of the present invention. Moreover, the equation $K=B^a=a^b$ does not represent a key sharing method based on ID information, but instead represents a primitive element of a finite field, which is not even a point on an algebraic curve. The term "inverse numeric values" is used in applicant's claims in the context that the relation between a shared key generated by a user A and a shared key generated by a user B is expressed by an inverse numeric value, not that a and b are symmetric.

With reference to claim 10, paragraph 21 of the Action asserts that Miyaji discloses "pairing defined on an algebraic curve is used to share a key/Weil pairing (Col. 13, line 40)". Applicant disagrees. This portion of Miyaji does not mention key sharing but, instead, describes how to extend a MOV attack, which is an attacking method of elliptic curve cryptosystem. For example, column 13, line 8, states "So we extend the MOV reduction as follows." Col. 13, line 31, states "Now we summarize the extended reducing method as follows." Weil pairing is used in this case to reduce a discrete logarithm problem on an elliptic curve to a discrete logarithm problem on a finite field. Such an attack is sometimes effective because there are cases where solving a discrete logarithm problem on a finite field is easier than solving a discrete logarithm problem on an elliptic curve. Bilinear mapping, as expressly claimed in claim 10 of the present invention, has no relevant use for Miyaji's method.

For these reasons, claims 3, 5, 6 and 8-11 should not be considered obvious over Tanaka in view of Miyaji. Hence, the rejections under 35 USC 103(a) should be withdrawn.

Conclusion

This application is believed to be in condition for allowance. The examiner is urged to telephone the undersigned to resolve any issues that remain after entry of this amendment. Any fees due with this response may be charged to our Deposit Account No. 50-1314.

Respectfully submitted,
HOGAN & HARTSON L.L.P.

Date: July 18, 2005

By:_____
Troy M. Schmelzer
Registration No. 36,667
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Phone: 213-337-6700
Fax: 213-337-6701